

DEPARTMENT OF HUMAN SERVICES POLICY AND PROCEDURES		
Reference: 01-11	Effective Date: June 15, 2010	Page: 1 of 3
SUBJECT: FACILITY SECURITY		

RATIONALE: It is the policy of the Department of Human Services that all Divisions, Offices, and Institutions must develop and maintain plans to control access to DHS employee work space and state and personal property. The Department of Human Services employees have both electronic and hard copy access to confidential information protected by government law and controlled access is crucial to ensure information security.

SCOPE: This policy applies to all Divisions, Offices and Institutions within the Department of Human Services. Agency management will assess the physical security of all of their facilities and report annually to the Executive Director. The assessment will include security breaches and new security measures implemented during the past year to mitigate past breaches in security.

PURPOSE: The purpose of this policy is to formalize the Facility Security Program of the Department of Human Services and provide guidelines for the development, maintenance and auditing of physical facility security. More importantly, the policy seeks to provide for the security of employees, confidential information, and state and personal property.

FACILITY SECURITY PROGRAM

The Department of Human Services recognizes the potential exposures associated with compromising security of confidential information and state and personal property.

The Facility Security Program is intended to provide a framework for constructing plans to ensure the safety of clients and employees with the control of access to employee work space. The plans resulting from this Program will include detailed descriptions of when they are to be implemented and who is responsible for their execution.

Division/Office/Institution Directors and accountable managers must identify and prioritize functions and services for which access by public is necessary in order to maintain normal business operations. Plans must detail responsibilities and tasks for controlling access and for securing employee work space.

RESPONSIBILITY

1. Bureau of Administrative Support - The Bureau of Administrative Support (BAS) will assist Divisions/Offices/Institutions to establish procedures to ensure physical security of all facilities, and that will restrict access to employee work space.

a. The Bureau of Administrative Support's responsibilities include:

- (1) Assist Division/Office/Institution Directors and accountable managers to prioritize security needs and acquire funding through Division/Office/Institution funds or the capital improvement process for construction necessary for securing employee work areas.
- (2) Conduct periodic audits of facilities and provide a written report of findings to Division/Office/Institution Directors and accountable managers.
- (3) Report annually on the status of the Department's preparedness to the Executive Director and Leadership Team.
- (4) Provide a methodology to follow in the event of a loss for recording, tracking, and reporting to the Division of Risk Management.

DEPARTMENT OF HUMAN SERVICES POLICY AND PROCEDURES		
Reference: 01-11	Effective Date: June 15, 2010	Page: 2 of 3
SUBJECT: FACILITY SECURITY		

(5) Coordinate with other Departments with whom Human Services has a working relationship to ensure that security plans do not conflict.

b. The BAS Region Managers responsibilities include:

(1) Identify facilities that are not secure and work with Division/Office/Institution Directors and accountable managers to identify and develop restricted access areas.

(2) Document and report effectiveness of the plans.

2. Division/Office/Institution Directors - Division/Office/Institution Directors will enforce overall compliance with the Department's Facility Security Program's guidelines.

a. The Division/Office/Institution Directors' responsibilities include:

(1) Develop and maintain a plan to control access to employee work space and state and personal property and information.

(2) Establish guidelines for disciplinary actions for employees who do not comply with the policy.

(3) Designate an individual to coordinate the Facility Security program for the Division/Office/Institution.

(4) Oversee the Facility Security plan; evaluate and approve the plans developed.

b. Division/Office/Institution designee responsibilities include:

(1) Coordinate the Facility Security for the Division/Office/Institution.

(2) Document and present plan status to accountable Director.

(4) Report the effectiveness of the plans to the BAS Region Manager after a security breach or security audit.

PLANNING STANDARD

This Standard establishes the basis for Facility Security planning throughout the Department of Human Services. This Standard applies to all Department locations, business operations, and employees.

IMPLEMENTATION REQUIREMENTS

Plans should address the resources needed to restrict access to employee work areas. The resources should include requirements for workspace, telecommunications, computer hardware, confidential files, state and personal assets and supplies.

1. Plan Development – The following should be included when considering plan development:

a. Division/Office/Institution goals and objectives, overall and specifically to secure facilities.

b. Detail procedures to escort clients in all restricted areas. (Non-DHS personnel should not be un-escorted in restricted areas.)

c. Procedures to keep "employee only" entrances locked and free of door hold open devices at all times.

d. Procedures for public to communicate with staff when a receptionist is not available.

e. Detail procedures to keep confidential documents locked up when unattended for any period of time.

f. Procedures to secure computers, all portable electronics including cell phones, laptops, PDA's and other devices used for state business, when not in use or unattended.

g. Procedures to secure personal possessions and information.

The result of the above plan development will provide a base for each Division, Office, and Institution to build a detailed plan.

DEPARTMENT OF HUMAN SERVICES POLICY AND PROCEDURES		
Reference: 01-11	Effective Date: June 15, 2010	Page: 3 of 3
SUBJECT: FACILITY SECURITY		

2. **Security Strategies** - For each security process, strategies must be developed that address the following considerations:

- a. Minimally acceptable access requirements
- b. Points of failure which will compromise confidentiality and security of state and personal assets.
- c. Each strategy that is developed to overcome a defined failure point must:
 - (1) Be attainable.
 - (2) Have a high probability of success.
 - (3) Be verifiable via audits.
 - (4) Be cost-effective.

The result of the above process will be a number of plans consisting of a series of tasks with staffing identified for each task, as well as associated costs, resources, and timelines.

3. **Plan Training and Exercising** - As a minimum, each Division/Office/Institution must:

- a. Provide training for all staff.
- b. Adjust plans according to the results of the annual audit.

4. **Plan Maintenance** - As a minimum, each Division/Office/Institution must:

- a. Review all plans at least annually to ensure they still meet the needs of the agency.
- b. Document and submit all plan changes as they occur to the BAS Region Manager.

DATE: 06-15-10



Lisa-Michele Church, Executive Director
Department of Human Services